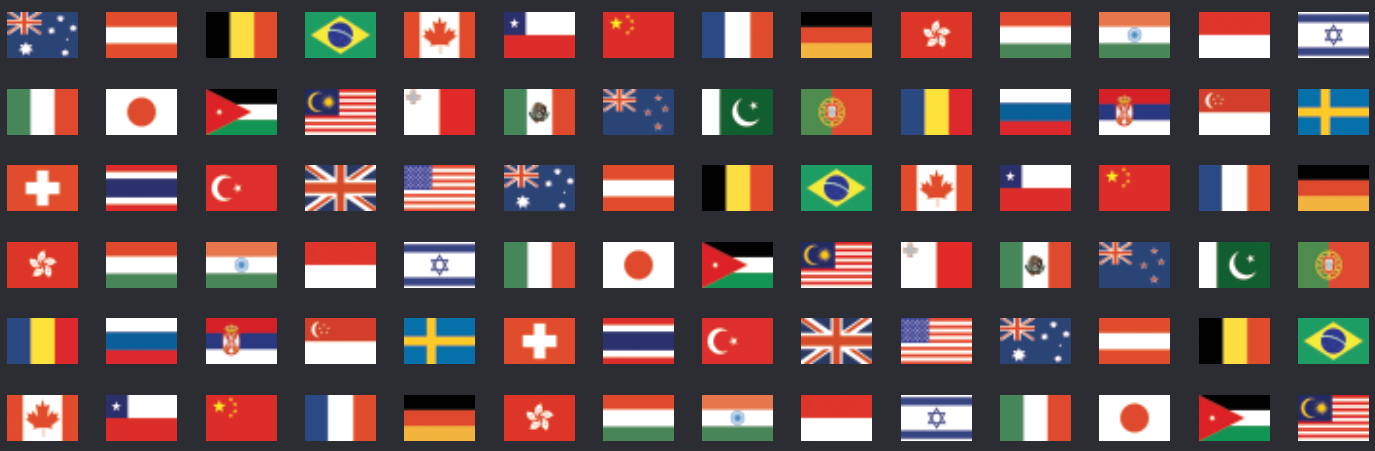
Data Protection & Privacy 2022

Contributing editors
Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

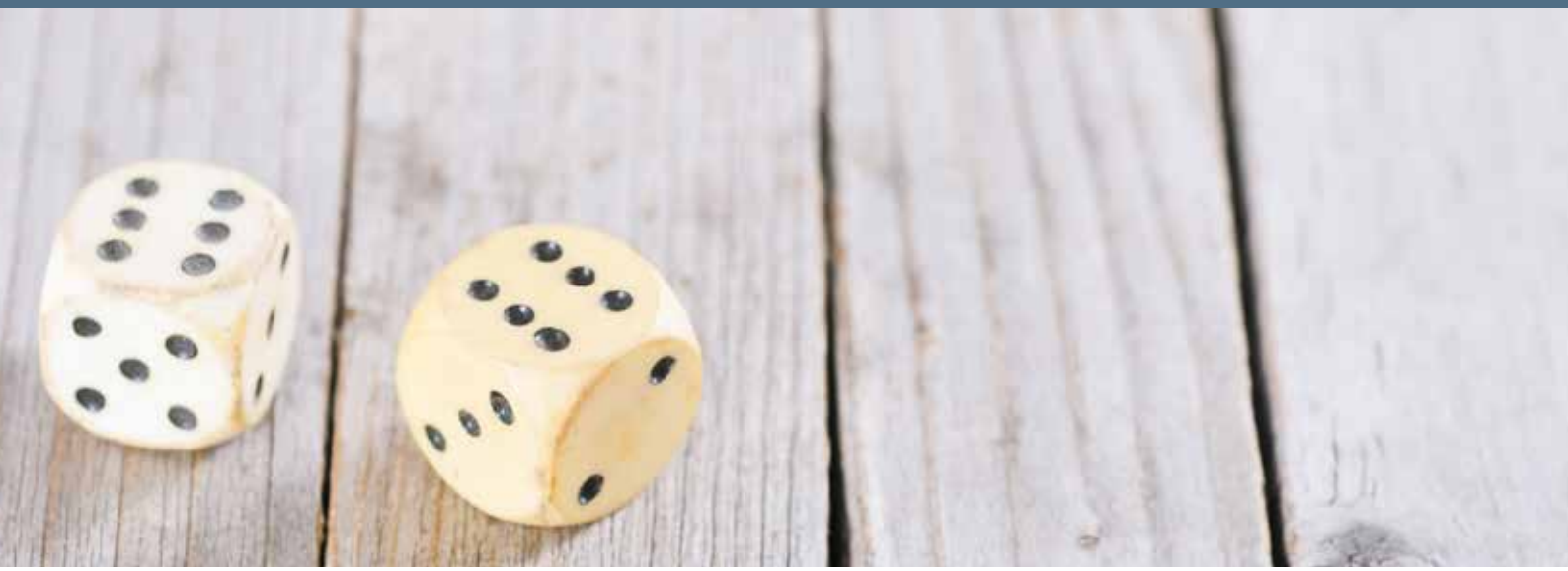


LEXOLOGY
Getting The Deal Through

HUNTON
ANDREWS KURTH

HUNTON
ANDREWS KURTH

Leaders in Handling High-Stakes Cybersecurity Events



Luck is not a strategy.

Increase your company's resilience and responsiveness to cyber attacks.

Hunton Andrews Kurth LLP's privacy and cybersecurity practice assists global organizations in managing data through every step of the information life cycle. We help businesses prepare for and respond to cybersecurity incidents all over the world. The firm is ranked as a top law firm globally for privacy and data security.

For more information, visit www.huntonprivacyblog.com.

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Senior business development manager
Adam Sargent
adam.sargent@gettingthedealthrough.com

Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

First published 2012
Tenth edition
ISBN 978-1-83862-644-0

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

Data Protection & Privacy

2022

Contributing editors
Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

Lexology Getting The Deal Through is delighted to publish the tenth edition of *Data Protection & Privacy*, which is available in print and online at www.lexology.com/gtdt.

Lexology Getting The Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique Lexology Getting The Deal Through format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes new chapters on Jordan, Pakistan and Thailand.

Lexology Getting The Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.lexology.com/gtdt.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Lexology Getting The Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors, Aaron P Simpson and Lisa J Sotto of Hunton Andrews Kurth LLP, for their continued assistance with this volume.

LEXOLOGY
Getting The Deal Through

London
July 2021

Reproduced with permission from Law Business Research Ltd
This article was first published in August 2021
For further information please contact editorial@gettingthedealthrough.com

Contents

United States

Aaron P Simpson and Lisa J Sotto

Hunton Andrews Kurth LLP

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

The US' legislative framework for the protection of PII historically has resembled a patchwork quilt. Unlike other jurisdictions, the United States does not have a single dedicated data protection law at the federal level, but instead regulates privacy primarily by industry, on a sector by sector basis. There are numerous sources of privacy law in the United States, including laws and regulations developed at both the federal and state levels. These laws and regulations may be enforced by federal and state authorities, and many provide individuals with a private right to bring lawsuits against organisations they believe are violating the law. Starting in 2018, increased legislative activity at the state level signalled a shift in focus towards more broad-based consumer privacy legislation in the United States. California became the first state to enact such legislation with the passage of the California Consumer Privacy Act (CCPA), a broad privacy law inspired in part by the General Data Protection Regulation (GDPR) in the European Union that is aimed at protecting the personal information of consumers across industries. Since then, numerous other states have proposed similarly broad privacy legislation, while multiple comprehensive privacy bills have been introduced at the federal level in the US Congress.

Data protection authority

2 Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

There is no single regulatory authority dedicated to overseeing data protection law in the United States. At the federal level, the regulatory authority responsible for oversight depends on the law or regulation in question. In the financial services context, for example, the Consumer Financial Protection Bureau and various financial services regulators (as well as state insurance regulators) have adopted standards under the Gramm-Leach-Bliley Act (GLB) that dictate how firms subject to their regulation may collect, use and disclose non-public personal information. Similarly, in the healthcare context, the Department of Health and Human Services is responsible for enforcement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Outside of the regulated industries context, the Federal Trade Commission (FTC) is the primary federal privacy regulator in the United States. Section 5 of the FTC Act, which is a general consumer protection law that prohibits 'unfair or deceptive acts or practices in or affecting commerce', is the FTC's primary enforcement tool in the privacy arena. The FTC has used its authority under section 5 to bring numerous privacy enforcement actions for a wide range of alleged violations by entities whose information practices have been deemed 'deceptive' or 'unfair'. Although section 5 does not give the FTC fining authority, it does enable it to bring enforcement actions against alleged violators, and these enforcement actions typically have resulted in consent decrees that prohibit the company from future misconduct and often require audits biennially for up to 20 years. Under section 5, the FTC can fine businesses that have violated a consent order.

At the state level, attorneys general can also bring enforcement actions for unfair or deceptive trade practices, or to enforce violations of specific state privacy laws. The California attorney general, for example, is empowered to enforce violations of the CCPA. Some state privacy laws allow affected individuals to bring lawsuits to enforce violations of the law.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

There are no regulations or structures that require the various federal and state data protection authorities to cooperate with one another. In the event of a data breach, however, many state attorneys general set up multistate task forces to pool resources, investigate the companies that experienced the breach, and reach a settlement or collectively litigate against the company. The resolutions often require companies to improve their information security programmes and obtain third-party assessments of their programmes.

Breaches of data protection

4 Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

In general, violations of federal and state privacy laws lead to civil, not criminal, penalties. The main exceptions are the laws directed at surveillance activities and computer crimes. Violations of the federal Electronic Communications Privacy Act (which is composed of the Wiretap Act, the Stored Communications Act and the Pen Register Act) or the Computer Fraud and Abuse Act can lead to criminal sanctions and civil liability. Also, many states have enacted surveillance laws that include criminal sanctions, in addition to civil liability, for violations.

Outside of the surveillance context, the US Department of Justice is authorised to criminally prosecute serious HIPAA violations. In circumstances where an individual knowingly violates restrictions on obtaining and disclosing legally cognisable health information, the Department of Justice may pursue criminal sanctions.

SCOPE

Exempt sectors and institutions

5 | Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

There is no single regulatory authority dedicated to overseeing data protection law in the United States. At the federal level, different privacy requirements apply to different industry sectors and data processing activities. These laws often are narrowly tailored and address specific data uses. For those entities not subject to industry specific regulatory authority, the Federal Trade Commission (FTC) has broad enforcement authority at the federal level, and attorneys general at the state level, to bring enforcement action for unfair or deceptive trade practices in the privacy context.

Communications, marketing and surveillance laws

6 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

Interception of communications is regulated primarily at the federal level by the Electronic Communications Privacy Act, which is composed of the Wiretap Act, the Stored Communications Act and the Pen Register Act. The federal Computer Fraud and Abuse Act also prohibits certain surveillance activities but is focused primarily on restricting other computer-related activities pertaining to hacking and computer trespass. At the state level, most states have laws that regulate the interception of communications.

There are only a handful of laws that specifically target the practice of electronic marketing and the relevant laws are specific to the marketing channel in question. Commercial email is regulated at the federal level by the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM). There are also state laws regulating commercial email, but these laws are generally pre-empted by CAN-SPAM. Telemarketing is regulated at the federal level by the Telephone Consumer Protection Act of 1991 (TCPA) and the Telemarketing and Consumer Fraud and Abuse Prevention Act, as well as regulations implemented by the FTC and the Federal Communications Commission (FCC). There are also state laws regulating telemarketing activities. Text message marketing is regulated primarily by the TCPA and regulations implemented by the FCC. Fax marketing is regulated by the TCPA, as amended by the Junk Fax Prevention Act of 2005, and state laws.

Other laws

7 | Identify any further laws or regulations that provide specific data protection rules for related areas.

In addition to the laws mentioned earlier, numerous other federal and state laws address privacy issues, including state information security laws and laws that apply to:

- consumer report information: Fair Credit Reporting Act and the Fair and Accurate Credit Transactions Act of 2003;
- children's information: Children's Online Privacy Protection Act;
- driver's information: Driver's Privacy Protection Act of 1994;
- video rental records: Video Privacy Protection Act; and
- federal government activities: Privacy Act of 1974.

The Cybersecurity Information Sharing Act (CISA) authorises entities to engage in certain cybersecurity monitoring, defence practices and information-sharing activities for purposes of protecting against cybersecurity threats. To help companies secure their information and systems, CISA provides businesses with certain liability protections in connection with monitoring information systems for cybersecurity purposes, implementing cybersecurity defensive measures, and sharing cyber intelligence with other private entities and federal government agencies.

In 2018, the California legislature enacted the California Consumer Privacy Act (CCPA), which became effective on 1 January 2020. The Act applies to any for-profit business that:

- does business in California;
- collects consumers' personal information (or on whose behalf such information is collected);
- alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information; and
- satisfies certain revenue thresholds or collects the personal information of 50,000 or more consumers, households or devices.

The CCPA defines 'personal information' broadly and contains provisions granting California consumers certain rights concerning their personal information. This new legislation in California has helped set the stage for several similar proposed laws currently pending in various state legislatures across the United States, as well as a possible federal data privacy law.

PII formats

8 | What forms of PII are covered by the law?

The United States does not have a dedicated data protection law. Thus, the definition of PII varies depending on the underlying law or regulation. In the state security breach notification law context, for example, the definition of PII generally includes an individual's name plus his or her social security number, driver's licence number, or financial account number. Some states broaden the definition of PII under the data breach notification laws to include elements such as medical information, insurance information, biometrics, email addresses and passwords to online accounts. In other contexts, such as FTC enforcement actions, the Gramm-Leach-Bliley Act or the Health Insurance Portability and Accountability Act of 1996, the definition of PII is much broader. Although certain laws apply only to electronic PII, many cover PII in any medium, including hard-copy records.

The CCPA contains a broad definition of PII that includes any 'information that identifies, relates to, describes, is reasonably capable of being associated with or could reasonably be linked, directly or indirectly, with a particular consumer or household'.

Extraterritoriality

9 | Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

As a general matter, the reach of US privacy laws is limited to organisations that are subject to the jurisdiction of US courts as constrained by constitutional due process considerations. Determinations regarding such jurisdiction are highly fact-specific and depend on the details of an organisation's contacts with the United States.

Covered uses of PII

10 | Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide PII processing services to owners? Do owners', controllers' and processors' duties differ?

Generally, US privacy laws apply to all processing of PII. There are no formal designations of 'controllers' and 'processors' under existing US law as there are in the laws of other jurisdictions. There are, however,

specific laws that set forth different obligations based on whether an organisation would be considered a data owner or a service provider. The most prominent example of this distinction is found in the US state breach notification laws. Pursuant to these laws, it is generally the case that the owner of the PII is responsible for notifying affected individuals of a breach, whereas a service provider is responsible for informing the data owner that it has suffered a breach affecting the data owner's data. Once a data owner has been notified of a breach by a service provider, the data owner, not the service provider, then must notify affected individuals.

The CCPA has adopted a concept quite similar to the controller concept under the EU General Data Protection Regulation, in that businesses directly subject to the law are defined to mean those entities who determine the purposes and means of the processing of consumers' personal Information.

LEGITIMATE PROCESSING OF PII

Legitimate processing – grounds

11 Does the law require that the holding of PII be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

US privacy laws generally do not limit the retention of PII to certain specified grounds. There are, however, laws that may indirectly affect an organisation's ability to retain PII. For example, organisations that are collecting personal information online from California residents must comply with the California Online Privacy Protection Act. Pursuant to this law, and general consumer expectations in the United States, the organisation must provide a privacy notice detailing the PII the company collects and how it is used. If the organisation uses the PII in materially different ways than those outlined in the privacy notice without providing notice and obtaining consent for such uses from the relevant consumers, these uses would likely be considered a deceptive trade practice under federal and state unfair competition laws. Similar laws are in place in Delaware and Nevada.

Legitimate processing – types of PII

12 Does the law impose more stringent rules for specific types of PII?

Since the United States does not have a dedicated data protection law, there is no singular concept of 'sensitive data' that is subject to heightened standards. There are, however, certain types of information that generally are subject to more stringent rules, which are described below.

Sensitive data in the security breach notification context

To the extent an organisation maintains individuals' names plus their social security numbers, driver's licence numbers or financial account numbers, notification generally is required under state and federal breach notification laws to the extent the information has been acquired or accessed by an unauthorised third party. Some states include additional data elements that could trigger breach notification. These include medical information, insurance information, biometrics, email addresses, and passwords to online accounts.

Consumer report information

The Fair Credit Reporting Act (FCRA) seeks to protect the confidentiality of information bearing on the creditworthiness and standing of consumers. The FCRA limits the permissible purposes for which reports that contain such information (known as consumer reports) may be disseminated, and consumer reporting agencies must verify that anyone requesting a consumer report has a permissible purpose for receiving the report.

Background screening information

Many sources of information used in background checks are considered public records in the United States, including criminal, civil court, bankruptcy, tax lien, professional licensing, workers' compensation and driving records. The FCRA imposes restrictions on the inclusion of certain public records in background screening reports when performed by consumer reporting agencies. Employers also can investigate job applicants and employees using internet search engines, but they must comply with their legal obligations under various labour and employment laws to the extent such laws restrict the use of the information. For instance, consideration of factors such as age, race, religion, disability, or political or union affiliation in making employment decisions can be the basis for a claim of unlawful discrimination under federal or state law.

Health information

Health Insurance Portability and Accountability Act of 1996 (HIPAA) specifies permissible uses and disclosures of protected health information (PHI), mandates that HIPAA-covered entities provide individuals with a privacy notice and other rights, regulates covered entities' use of service providers (known as business associates), and sets forth extensive information security safeguards relevant to electronic PHI.

Children's information

Children's Online Privacy Protection Act (COPPA) imposes extensive obligations on organisations that collect personal information from children under 13 years of age online. COPPA's purpose is to provide parents and legal guardians greater control over the online collection, retention and disclosure of information about their children.

Under the Privacy Rights for California Minors in the Digital World law, California minors who are registered users of a website, online service or mobile application may seek the removal of content and information that the minors have posted. A 'minor' is defined as a California resident under the age of 18.

The California Consumer Privacy Act of 2018 prohibits a business from selling a minor's personal information unless:

- the consumer is between 13 and 16 years of age and has affirmatively authorised the sale (ie, they opt-in); or
- the consumer is less than 13 years of age and the consumer's parent or guardian has affirmatively authorised the sale.

Biometric information

Illinois, Texas and Washington have enacted biometric privacy laws that set forth requirements for businesses that collect and use biometric information for commercial purposes. These laws generally require that companies must provide notice to individuals and obtain their affirmative consent before using their biometric identifiers for commercial purposes. The laws also require companies to implement security measures to protect the biometric information they maintain and to retain the biometric identifiers for no longer than necessary to comply with the law, protect against fraud, criminal activity, security threats or liability, or to provide the service for which the biometric identifier was collected.

State social security number laws

Numerous state laws impose obligations concerning the processing of state social security numbers (SSNs). These laws generally prohibit:

- intentionally communicating SSNs to the general public;
- using SSNs on identity cards required for individuals to receive goods or services;
- requiring that SSNs be used in internet transactions unless the transaction is secure or the SSN is encrypted or redacted;

- requiring an individual to use an SSN to access a website unless another authentication device is also used; and
- mailing materials with SSNs (subject to certain exceptions).

Several state laws also impose restrictions targeting specific SSN uses.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PII

Notification

13 Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

For organisations not otherwise subject to specific regulation, the primary law requiring them to provide a privacy notice to consumers is California Online Privacy Protection Act. This law requires a notice when an organisation collects personal information from individuals in the online and mobile contexts. The law requires organisations to specify in the notice:

- the categories of PII collected through the website;
- the categories of third-party persons or entities with whom the operator may share the PII;
- the process an individual must follow to review and request changes to any of his or her PII collected online, to the extent such a process exists;
- how the operator responds to web browser 'do-not-track' signals or similar mechanisms that permit individuals to exercise choice regarding the collection of their PII online over time and across third-party websites or online services, if the operator engages in such collection;
- whether third parties collect PII about individuals' online activities over time and across different websites when an individual uses the operator's website or online service;
- the process by which consumers who visit the website or online service are notified of material changes to the privacy notice for that website; and
- the privacy notice's effective date.

Delaware and Nevada have also enacted laws that require operators of commercial internet services to provide similar information to their users when collecting PII online.

The California Consumer Privacy Act (CCPA) also imposes specific privacy notice disclosure requirements, which apply to personal information collected both online and offline. For example, businesses must provide notice to consumers of their rights under the CCPA (eg, the right to opt-out of the sale of personal information) and how to exercise those rights. The CCPA also requires a business to include the following in its privacy notice:

- a list of the categories of personal information collected about consumers in the preceding 12 months;
- the categories of sources from which the personal information was collected;
- the business or commercial purpose for collecting or selling the information;
- the categories of third parties with whom the personal information is shared; and
- lists of the categories of personal information sold and disclosed about consumers if the business sells consumers' personal information or discloses it to third parties for a business purpose.

If the business sells personal information, it must provide a clear and conspicuous link on their website that says 'Do not sell my personal information' and provide consumers with a mechanism to opt-out of the sale of their personal information, a decision the business must respect. Companies must update their notices at least once every 12 months. The CCPA also imposes a limited notice obligation in the employment context.

In addition to the California, Delaware and Nevada laws, other federal laws require a privacy notice to be provided in certain circumstances, such as the following.

Children's Online Privacy Protection Act

Under the Children's Online Privacy Protection Rule of the Federal Trade Commission (FTC), implemented under the Children's Online Privacy Protection Act (COPPA), operators of websites or online services that are directed to children under 13 years old, or who knowingly collect information from children online, must provide a conspicuous privacy notice on their site. The notice must include statutorily prescribed information, such as the types of personal information collected, how the operator will use the personal information, how the operator may disclose the personal information to third parties, and details regarding a parent's ability to review the information collected about a child and opt-out of further information collection and use. In most cases, an operator that collects information from children online also must send a direct notice to parents that contains the information set forth above along with a statement that informs parents the operator intends to collect the personal information from their child. The operator also must obtain verifiable parental consent before collecting, using or disclosing personal information from children.

Fair Credit Reporting Act and Fair and Accurate Credit Transactions Act

The Fair Credit Reporting Act (FCRA), as amended by the Fair and Accurate Credit Transactions Act of 2003 (FACTA), imposes several requirements on consumer reporting agencies to provide consumers with notices, including in the context of written disclosures made to consumers by a consumer reporting agency, identity theft, employment screening, pre-screened offers of credit or insurance, information sharing with affiliates, and adverse actions taken based on a consumer report.

Gramm-Leach-Bliley Act

Financial institutions must provide an initial privacy notice to customers by the time the customer relationship is established. If the financial institution shares non-public personal information with non-affiliated third parties outside of an enumerated exception, the entity must provide each relevant customer with an opportunity to opt-out of the information sharing. Following this initial notice, financial institutions subject to the Gramm-Leach-Bliley Act (GLB) must provide customers with an annual notice. The annual notice is a copy of the full privacy notice and must be provided to customers each year for as long as the customer relationship persists. For 'consumers' (individuals that have obtained a financial product or service for personal, family or household purposes but do not have an ongoing, continuing relationship with the financial institution), a notice generally must be provided before the financial institution shares the individual's non-public personal information with third parties outside of an enumerated exception. A GLB privacy notice must explain what non-public personal information is collected, the types of entities with whom the information is shared, how the information is used, and how it is protected. The notice also must indicate the consumer's right to opt-out of certain information sharing with non-affiliated parties. In 2009, the federal financial regulators responsible for enforcing privacy regulations implemented pursuant to GLB released model forms for financial institutions to use when developing their privacy notices. Financial institutions that use the model form in a manner consistent with the regulators' published instructions are deemed compliant with the

regulation's notice requirements. In 2011, the Dodd-Frank Wall Street Reform and Consumer Protection Act transferred the GLB privacy notice rule-making authority from the financial regulatory agencies to the Consumer Financial Protection Bureau (CFPB). The CFPB then restated the GLB implementing regulations, including those pertaining to the model form, in Regulation P.

Health Insurance Portability and Accountability Act

The Privacy Rule promulgated under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires covered entities to provide individuals with a notice of privacy practices. The Rule imposes several content requirements, including:

- the covered entities' permissible uses and disclosures of protected health information (PHI);
- the individual's rights concerning the PHI and how those rights may be exercised;
- a list of the covered entity's statutorily prescribed duties concerning the PHI; and
- contact information for the individual at the covered entity responsible for addressing complaints regarding the handling of PHI.

Exemption from notification

14 | When is notice not required?

Notice would not be required if a business is subject to specifically regulated scenarios.

Control of use

15 | Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

In the regulated contexts discussed above, individuals are provided with limited choices regarding the use of their information. The choices are dependent upon the underlying law. Under the GLB, for example, customers and consumers have a legal right to opt out of having their non-public personal information shared by a financial institution with third parties (outside an enumerated exception). Similarly, under the FCRA, as amended by FACTA, individuals have a right to opt-out of having certain consumer report information shared by a consumer reporting agency with an affiliate, in addition to another opt-out opportunity before any use of a broader set of consumer report information by an affiliate for marketing reasons. Federal telemarketing laws and the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 Act give individuals the right to opt-out of receiving certain types of communications, as do similar state laws.

Also, California's Shine the Light Law requires companies that collect personal information from residents of California generally to either provide such individuals with an opportunity to know which third parties the organisation shared California consumers' personal information with for such third parties' direct marketing purposes during the preceding calendar year or, alternatively, to give the individuals the right to opt-out of such third-party sharing. This right is expanded in the CCPA, which provides that, upon request from a California consumer, an organisation must disclose:

- the categories and specific pieces of personal information the business has collected about the consumer;
- the categories of sources from which the personal information is collected;
- the business or commercial purposes for collecting or selling personal information;
- the categories of third parties with whom the business shares personal information;
- if applicable, the categories of personal information about the consumer the business has disclosed for a business purpose and the categories of third parties to whom each category of personal information was disclosed; and
- if applicable, the categories of personal information about the consumer the business has sold and the categories of third parties to whom each category of personal information was sold.

Under the CCPA, a consumer also has the right to request that a business delete any personal information about the consumer, which the business has collected from the consumer. The CCPA also provides consumers with the right to opt-out of the sale of their personal information.

As the primary regulator of privacy issues in the United States, the FTC periodically issues guidance on pressing issues. In the FTC's 2012 report titled 'Protecting Consumer Privacy in an Era of Rapid Change', the FTC set forth guidance indicating that organisations should provide consumers with choices concerning uses of personal information that are inconsistent with the context of the interaction through which the organisation obtained the personal information. In circumstances where the use of the information is consistent with the context of the transaction, the FTC indicated that offering such choices is not necessary.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PII?

There is no existing law of general application in the United States that imposes standards related to the quality, currency and accuracy of PII. There are laws, however, in specific contexts that contain standards intended to ensure the integrity of personal information maintained by an organisation. The FCRA, for example, requires users of consumer reports to provide consumers with notices if the user will be taking an adverse action against the consumer based on information contained in a consumer report. These adverse action notices must provide the consumer with information about the consumer's right to obtain a copy of the consumer report used in making the adverse decision and to dispute the accuracy or completeness of the underlying consumer report. Similarly, under the HIPAA Security Rule, covered entities must ensure, among other things, the integrity of electronic PHI.

Amount and duration of data holding

17 | Does the law restrict the amount of PII that may be held or the length of time it may be held?

Existing US privacy laws generally do not impose direct restrictions on an organisation's retention of personal information. There are, however, thousands of records retention laws at the federal and state level that impose specific obligations on how long an organisation may (or must) retain records, many of which cover records that contain personal information.

Finality principle

18 | Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

US privacy laws have not specifically adopted the finality principle. As a practical matter, organisations typically describe their uses of personal information collected from consumers in their privacy notices. To the extent an organisation uses the personal information it collects subject to such a privacy notice for materially different purposes than those outlined in the notice, such a practice would likely be considered a deceptive trade practice under federal and state consumer protection laws.

Use for new purposes

19 If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

In the United States, organisations must use the personal information they collect in a manner that is consistent with any privacy representations it has made in their privacy notices or otherwise. To the extent an organisation would like to use previously collected personal information for a materially different purpose, the FTC and state attorneys general would expect the organisation to first obtain opt-in consent from the consumer for such use. Where the privacy notice is required by a statute (eg, a notice to parents under COPPA), failure to handle the PII as described pursuant to such notice also may constitute a violation of the statute.

SECURITY

Security obligations

20 What security obligations are imposed on PII owners and service providers that process PII on their behalf?

Similar to privacy regulation, there is no comprehensive federal information security law in the United States. Accordingly, the security obligations that are imposed on data owners and entities that process PII on their behalf depend on the regulatory context. These security obligations are set out below.

Gramm-Leach-Bliley Act

The Safeguards Rule implemented under the Gramm-Leach-Bliley Act requires financial institutions to 'develop, implement, and maintain a comprehensive information security program' that contains administrative, technical and physical safeguards designed to protect the security, confidentiality and integrity of customer information. The requirements of the Safeguards Rule apply to all non-public personal information in a financial institution's possession, including information about the institution's customers as well as customers of other financial institutions. Although the Safeguards Rule is not prescriptive in nature, it does set forth five key elements of a comprehensive information security programme:

- designation of one or more employees to coordinate the programme;
- conducting risk assessments;
- implementation of safeguards to address risks identified in risk assessments;
- oversight of service providers; and
- evaluation and revision of the programme in light of material changes to the financial institution's business.

Health Insurance Portability and Accountability Act

The Security Rule implemented under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which applies to electronically protected health information (ePHI), sets forth specific steps that covered entities and their service providers must take to:

- ensure the confidentiality, integrity, and availability of ePHI;
- protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI;
- protect against any reasonably anticipated uses or disclosures of ePHI; and
- ensure compliance with the Security Rule by the covered entity's workforce.

Unlike other US information security laws, the Security Rule is highly prescriptive and sets forth detailed administrative, technical and physical safeguards.

State information security laws

Laws in several US states, including California, impose general information security standards on organisations that maintain personal information. California's law, for example, requires organisations that own or license personal information about California residents to implement and maintain reasonable security procedures and practices to protect the information from unauthorised access, destruction, use, modification or disclosure. Also, organisations that disclose personal information to non-affiliated third parties must contractually require those entities to maintain reasonable security procedures.

Massachusetts Standards for the Protection of Personal Information

In 2008, Massachusetts issued regulations requiring any person who holds personal information about Massachusetts residents to develop and implement a comprehensive, written information security programme to protect the data. The regulations apply in the context of both consumer and employee information and require the protection of personal data in both paper and electronic formats. Unlike the California law, the Massachusetts law contains certain specific data security standards, including required technical safeguards, on all private entities with Massachusetts consumers or employees.

New York SHIELD Act

In 2019, New York enacted the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), which amended the state's existing data breach notification law to impose certain data security requirements on businesses that own or license computerised data that includes New York residents' 'private information'. The SHIELD Act requires businesses to develop, implement, and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information including, but not limited to, the disposal of such data. A business can comply with the SHIELD Act's 'reasonable safeguards' requirement by either being subject to and compliant with applicable federal or New York data security rules, regulations or statutes or implementing a data security programme that includes reasonable administrative, technical and physical safeguards.

New York Department of Financial Services Cybersecurity Regulation

In 2017, the New York State Department of Financial Services (NYDFS) issued a regulation that establishes a robust set of cybersecurity requirements for financial services providers regulated by the NYDFS. The cybersecurity regulation applies to entities that operate under a NYDFS licence, registration or charter pursuant to New York banking, insurance or financial services law. The cybersecurity regulation requires such covered entities to maintain a comprehensive cybersecurity programme and implement certain processes and technical controls related to risk assessments, user access privileges, software security, system auditing and monitoring, data encryption, data disposal and retention, and cybersecurity incident response. Also, the regulation assigns cybersecurity oversight responsibilities to senior officials and boards of directors and requires entities to report cybersecurity events to the NYDFS.

Nevada encryption law

Nevada law requires that organisations doing business in Nevada and that accept payment cards must comply with the Payment Card Industry Data Security Standard (PCI DSS). It requires that other organisations doing business in Nevada use encryption when transferring 'any personal information through an electronic, non-voice transmission other than a facsimile to a person outside of the secure system of the data collector', and moving 'any data storage device containing personal information beyond the logical or physical controls of the data collector or its data storage contractor'.

State social security number laws

Numerous state laws impose obligations concerning the processing of state social security numbers (SSNs). These laws generally prohibit:

- intentionally communicating SSNs to the general public;
- using SSNs on ID cards required for individuals to receive goods or services;
- requiring that SSNs be used in internet transactions unless the transaction is secure or the SSN is encrypted or redacted;
- requiring an individual to use an SSN to access a website unless another authentication device is also used; and
- mailing materials with SSNs (subject to certain exceptions).

Several state laws also impose restrictions targeting specific SSN uses.

Key industry and government standards

There are several key industry standards in the area of information security. The PCI DSS applies to all entities that process credit or debit cards. It obliges covered entities to comply with prescriptive information security requirements, which include:

- installing and maintaining a firewall configuration to protect cardholder data;
- encrypting the transmission of cardholder data across public networks;
- protecting systems against malware and regularly updating anti-virus software or programs; and
- restricting physical access to cardholder data.

Entities subject to the PCI DSS are required to validate their compliance on an annual basis. The specific requirements necessary to certify compliance depend on the type of entity involved in the processing of payment cards and the number of payment cards processed by the covered entity pursuant to each payment card brand's compliance validation programme.

The National Institute of Standards and Technology (NIST), which is part of the US Department of Commerce, has produced various publications and guidance on a host of information security topics that are intended to help businesses. The most significant of the NIST security publications is the NIST Cybersecurity Framework. This is a flexible document that gives users the discretion to decide which aspects of network security to prioritise, what level of security to adopt and which standards, if any, to apply. Other guidance documents address methods of media sanitisation, conducting risk assessments, security considerations in the information system development life cycle and storage encryption for end-user devices.

Also, the International Organization for Standardization (ISO) is a non-governmental organisation composed of the national standards institutes of 161 countries. The ISO sets international standards across a range of industries. In the area of information security, the ISO has promulgated two important standards: 27001 and 17799/27002. ISO 27001 provides a 'process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system'. It is a flexible standard, and users are encouraged to:

- understand their information security requirements and the need to establish policy objectives for information;
- implement controls to manage information security risks in the context of the organisation's overall business risks;
- monitor and review the performance and effectiveness of the Information Security Management System; and
- continually improve the Information Security Management System based on objective measurement.

Notification of data breach

21 Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

There are no breach notification laws of general application at the federal level. There are, however, numerous targeted breach notification laws at both the state and federal level, including:

State breach laws

At present, all 50 states, the District of Columbia, the US Virgin Islands, Guam and Puerto Rico have enacted breach notification laws that require data owners to notify affected individuals in the event of unauthorised access to or acquisition of personal information, as that term is defined in each law. In addition to notification of individuals, a majority of the state laws also require notice to a state regulator in the event of a breach, typically the state attorney general. Although most state breach laws require notification only if there is a reasonable likelihood that the breach will result in harm to affected individuals, several jurisdictions do not employ such a harm threshold and require notification of any incident that meets their definition of a breach.

Federal interagency guidance

Several federal banking regulators issued the Interagency Guidance on Response Programs for Unauthorised Access to Customer Information and Customer Notice. Entities regulated by the Office of the Comptroller of the Currency, the Federal Reserve Board, the Federal Deposit Insurance Corporation and the Office of Thrift Supervision are subject to the Interagency Guidance. The Interagency Guidance sets forth that subject financial institutions develop and implement a response programme to address incidents of unauthorised access to customer information processed in systems the institutions or their service providers use to access, collect, store, use, transmit, protect, or dispose of the information. Also, the Interagency Guidance contains three key breach notification requirements. First, when a financial institution becomes aware of an incident involving unauthorised access to or use of sensitive customer information, the institution must promptly notify its primary federal regulator. Second, the institution must notify appropriate law enforcement authorities in situations involving federal criminal violations requiring immediate attention. Third, the institution also must notify relevant customers of the incident if the institution's investigation determines that misuse of sensitive customer information has occurred or is reasonably possible. In this context, 'sensitive customer information' means a customer's name, address, or telephone number in conjunction with the customer's SSN, driver's licence number, account number, credit or debit card number, or a PIN or password that would permit access to the customer's account. Any combination of these data elements that would allow an unauthorised individual to access the customer's account also would constitute sensitive customer information.

Health Information Technology for Economic and Clinical Health Act

The information security breach provisions in the Health Information Technology for Economic and Clinical Health Act (HITECH Act) apply in the healthcare context, governing both HIPAA-covered entities and non-HIPAA covered entities. The HITECH Act and the breach-related provisions of the Department of Health and Human Services regulations implementing the Act require HIPAA-covered entities that experience an information security breach to notify affected individuals, and service providers of HIPAA-covered entities to notify the HIPAA-covered entity following the discovery of a breach. Unlike the state breach notification laws, the obligation to notify as a result of an information security

breach under the HITECH Act falls on any HIPAA covered entity that 'accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured [personal health information (PHI)]'. Any HIPAA-covered entity that processes unsecured PHI must notify affected individuals in the event of a breach, whether the covered entity owns the data or not.

INTERNAL CONTROLS

Data protection officer

22 | Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

No, the appointment of a data protection officer is not mandatory under the privacy rules of general application. Many organisations in the United States appoint a chief privacy officer (CPO), but his or her responsibilities are dictated by business need rather than legal requirements. Certain sector-specific laws do require the appointment of a CPO. For example, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires the appointment of a privacy official who is responsible for the development and implementation of the policies and procedures of the entity. Also, several federal and state laws require that a chief information security officer or an equivalent be appointed. These laws include the Gramm-Leach-Bliley Act (GLB), HIPAA and the New York State Department of Financial Services' Cybersecurity Regulations.

Record keeping

23 | Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

There are currently no legal requirements of general application that obligate owners of PII to maintain internal records or establish internal processes or documentation. Several statutory frameworks in the United States require organisations to develop an information security programme, which typically must contain internal processes and documentation. These include requirements imposed by the GLB, HIPAA and state information security laws.

New processing regulations

24 | Are there any obligations in relation to new processing operations?

Generally, there are no legal obligations concerning new processing operations, such as to apply a privacy by design approach or carry out privacy impact assessments. Applicable to US federal agencies only, the E-Government Act of 2002 requires the completion and publication of privacy impact assessments when the agency engages in a new collection of, or applies new technologies to, personally identifiable information. The Federal Trade Commission issued a report, however, that recommends that companies consider privacy by design principles during all stages of the design and development of products and services.

REGISTRATION AND NOTIFICATION

Registration

25 | Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

There are no generally applicable registration requirements for data processing activities in the United States.

Formalities

26 | What are the formalities for registration?

There are no generally applicable registration requirements for data processing activities in the United States.

Penalties

27 | What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

There are no generally applicable registration requirements for data processing activities in the United States.

Refusal of registration

28 | On what grounds may the supervisory authority refuse to allow an entry on the register?

There are no generally applicable registration requirements for data processing activities in the United States.

Public access

29 | Is the register publicly available? How can it be accessed?

There are no generally applicable registration requirements for data processing activities in the United States.

Effect of registration

30 | Does an entry on the register have any specific legal effect?

There are no generally applicable registration requirements for data processing activities in the United States.

Other transparency duties

31 | Are there any other public transparency duties?

There are no generally applicable registration requirements for data processing activities in the United States.

TRANSFER AND DISCLOSURE OF PII

Transfer of PII

32 | How does the law regulate the transfer of PII to entities that provide outsourced processing services?

As a general matter, organisations address privacy and information security concerns in their agreements with service providers that will provide outsourced processing services. There are no laws of general application in the United States that impose requirements on data owners concerning their service providers. There are, however, specific laws that address this issue, such as the following.

Health Insurance Portability and Accountability Act

Through the Privacy and Security Rules, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) imposes significant restrictions on the disclosure of protected health information (PHI). The regulations require covered entities to enter into business associate agreements containing statutorily mandated language before PHI may be disclosed to a service provider.

Gramm-Leach-Bliley Act

Under the Privacy Rule enacted pursuant to the Gramm-Leach-Bliley Act (GLB), before disclosing consumer non-public personal information to a service provider, a financial institution must enter into a contract with

the service provider prohibiting the service provider from disclosing or using the information other than to carry out the purposes for which the information was disclosed. Under the Safeguards Rule enacted under the GLB, before allowing a service provider access to customer personal information, the financial institution must take reasonable steps to ensure that the service provider is capable of maintaining appropriate safeguards, and require the service provider by contract to implement and maintain such safeguards.

State information security and privacy laws

Several states impose a general information security standard on businesses that maintain personal information. These states have laws requiring companies to implement reasonable information security measures. California law and Massachusetts law require organisations that disclose personal information to service providers to include contractual obligations that those entities maintain reasonable security procedures. The California Consumer Privacy Act (CCPA) prescribes additional content be included in contracts with service providers.

Restrictions on disclosure

33 | Describe any specific restrictions on the disclosure of PII to other recipients.

A wide variety of laws contain disclosure restrictions targeted to specific forms of PII. For example, HIPAA and the GLB impose limitations on certain disclosures, such as requirements for consent and contracts with certain types of recipients. The CCPA provides rights to consumers concerning a business's ability to sell their personal information to certain types of third parties.

Cross-border transfer

34 | Is the transfer of PII outside the jurisdiction restricted?

US privacy laws do not impose restrictions on cross-border data transfers.

Notification of cross-border transfer

35 | Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

US privacy laws do not impose restrictions on cross-border data transfers.

Further transfer

36 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

US privacy laws do not impose restrictions on cross-border data transfers.

RIGHTS OF INDIVIDUALS

Access

37 | Do individuals have the right to access their personal information held by PII owners? Describe how this right can be exercised as well as any limitations to this right.

There are no laws of general application in the United States that provide individuals with a right to access the personal information about them that is held by an organisation. There are specific laws that address access rights, such as the following.

Health Insurance Portability and Accountability Act

Under the Privacy Rule enacted under the Health Insurance Portability and Accountability Act of 1996, an individual has a right to access protected health information (PHI) about the individual that is maintained by the covered entity unless the covered entity has a valid reason for denying the individual such access. Valid reasons can include the fact that the PHI is subject to restricted access under other laws, or that access to the PHI is reasonably likely to cause substantial harm to another person. A covered entity must provide the requested access to the PHI within 30 days of the request and must explain the justification for any denial of access.

California's Shine the Light Law

Under this law, organisations that collect personal information from California residents generally must either:

- provide such individuals with an opportunity to know which third parties the organisation shared California consumers' personal information with for such third parties' direct marketing purposes during the prior calendar year; or
- allow such individuals the right to opt-out of most third-party sharing.

If an organisation implements the option in the first point above, it must provide California residents with a postal address, email address or freephone telephone or fax number that California residents may contact to obtain the list of relevant third parties. Organisations are required to respond only to a single request per California resident per calendar year.

California Consumer Privacy Act

Under this law, California consumers have a right to request information about the PII organisations collected, shared and sold within the past 12 months. Specifically, a consumer has a right to request that an organisation disclose:

- the categories of PII the organisation has collected about that consumer;
- the categories of sources from which the PII is collected;
- the business or commercial purpose for collecting or selling PII;
- the categories of third parties with whom the organisation shares PII;
- the specific pieces of PII it has collected about that consumer;
- the categories of PII it has sold about the consumer and the categories of third parties to whom the PII was sold; and
- the categories of PII that the organisation disclosed for a business purpose and the categories of third parties to whom the PII was disclosed for a business purpose.

The California Consumer Privacy Act (CCPA) also provides that an organisation's response to an access request must be delivered in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance.

Other rights

38 | Do individuals have other substantive rights?

The CCPA provides consumers with the right to request that a business delete the personal information about the consumer that the business has collected from the consumer and direct any service providers to delete the consumer's personal information. There are several enumerated exceptions to this deletion requirement, such as if it is necessary to maintain the consumer's personal information to complete the transaction for which the personal information was collected or to protect against malicious, deceptive, fraudulent or illegal activity.

Also, some sector-specific laws provide other substantive rights. For example, the Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 provides individuals with the right to amend their PHI. If an individual requests that a covered entity amend the individual's PHI, the covered entity must do so within 60 days of the request and must explain any reasons for denying the request. The Children's Online Privacy Protection Act allows parents or legal guardians to revoke their consent and refuse the further use or collection of personal information from their child. This law also allows parents or guardians to request the deletion of their child's personal information. The Fair Credit Reporting Act (FCRA) provides individuals with the right to dispute and demand correction of information about them that is held by consumer reporting agencies.

Compensation

39 Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Individuals are entitled to monetary damages for wrongful acts under common law and pursuant to most statutes that provide for a private right of action. Consumers often bring class-action lawsuits against organisations as a result of alleged privacy violations, such as statutory violations or other wrongful acts that affect them, such as information security breaches. In security breach cases, consumers often allege that the organisation was negligent in securing the consumers' personal information and that such negligence led to the security breach. As a general matter, consumers would need to establish that they suffered actual damages as a direct result of the organisation's negligence to succeed on their claim.

In the regulatory context, the ability to obtain monetary damages or compensation depends entirely on the statute in question. Under section 5 of the Federal Trade Commission Act (the FTC Act), for example, equitable relief is available first but then monetary penalties could reach US$41,484 per violation for a breach of a consent order. Under the FCRA, in the event an organisation is wilfully non-compliant with the law, the Act provides for the recovery by aggrieved individuals of actual damages sustained or damages of 'not less than US$100 and not more than US$1,000' per violation, plus punitive damages, attorneys' fees and court costs. Negligent non-compliance may result in liability for actual damages as well as costs and attorneys' fees. Other laws, such as section 5 of the FTC Act, provide no private right of action to individuals and instead can be enforced solely by the regulator.

Enforcement

40 Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

To the extent an individual obtains monetary relief as a result of illegal activity by an organisation, that relief will be obtained primarily through the judicial system. Typically, the civil penalties imposed by regulators are not paid directly to aggrieved individuals. There are, however, exceptions to this rule. For example, under the FCRA, organisations that settle claims with regulators can be asked to provide funds for consumer redress.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

41 Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

There is no law of general application regarding privacy and information security in the United States, and thus there are no derogations, exclusions or limitations of general application as there are in other jurisdictions. Cybersecurity Information Sharing Act (CISA) provides companies with liability protection for cybersecurity monitoring and defence practices. For example, CISA pre-empts state law and grants liability protection to companies against any cause of action in any court for the monitoring of an information system and information to the extent the monitoring is conducted for cyber-security purposes delineated under the CISA.

SUPERVISION

Judicial review

42 Can PII owners appeal against orders of the supervisory authority to the courts?

The ability of an organisation to appeal orders of a supervisory authority is highly contextual. In the Federal Trade Commission (FTC) context, an order is the result of an administrative proceeding before an FTC administrative law judge and the full FTC on review. An order issued by the FTC as a result of this process can be appealed directly to a federal court of appeals, where the FTC's order would be entitled to some deference on review.

SPECIFIC DATA PROCESSING

Internet use

43 Describe any rules on the use of 'cookies' or equivalent technology.

There have been numerous legislative efforts aimed at providing formal regulation for the use of cookies, particularly in the behavioural advertising context. To date, none of those legislative efforts has succeeded. The Federal Trade Commission (FTC) has issued a substantial amount of guidance in the area of online behavioural advertising, and the industry has responded with a series of self-regulatory frameworks. Although not focused directly on cookies, there have been several civil actions brought by individuals and regulatory enforcement actions brought by the FTC for practices that depend on the use of cookies, but the allegations tend to focus on laws of more general application, such as surveillance laws and section 5 of the FTC Act. At the state level, California law requires website operators to disclose how the operator responds to internet browser 'do not track' signals or other mechanisms that provide consumers with the ability to exercise choice regarding the collection of personal information about an individual consumer's online activities over time and across a third-party website or online services if the operator engages in that collection. Also, the California Consumer Privacy Act affords consumers certain rights concerning the sale of their data, which could bear an impact on the use of third-party cookies in many circumstances.

Electronic communications marketing

44 | Describe any rules on marketing by email, fax or telephone.

There are only a handful of laws that specifically target the practice of electronic marketing and the relevant laws are specific to the marketing channel in question. Commercial email is regulated at the federal level by the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM). There are also state laws regulating commercial email, but these laws are generally pre-empted by CAN-SPAM. Telemarketing is regulated at the federal level by the Telephone Consumer Protection Act of 1991 (TCPA) and the Telemarketing and Consumer Fraud and Abuse Prevention Act, as well as regulations implemented by the FTC and the Federal Communications Commission (FCC). There are also state laws regulating telemarketing activities. Text message marketing is regulated primarily by the TCPA and regulations implemented by the FCC. Fax marketing is regulated by the TCPA, as amended by the Junk Fax Prevention Act of 2005, and state laws.

Cloud services

45 | Describe any rules or regulator guidance on the use of cloud computing services.

The National Institute of Standards and Technology has issued guidelines on security and privacy in cloud computing that are directed at federal departments and agencies. The guidelines state that the cloud computing solution should be able to meet the specific privacy and security needs of the department or agency, and departments and agencies should remain accountable for the security and privacy of any data and applications maintained in the cloud. Also, the Department of Health and Human Services has issued guidance on the Health Insurance Portability and Accountability Act of 1996 and cloud computing, clarifying that covered entities and business associates must enter into business associate agreements with cloud service providers that store or process electronically protected health information (PHI) before storing records containing electronic PHI in a cloud computing facility.

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

In 2018, the California legislature enacted the ground-breaking California Consumer Privacy Act (CCPA), which signalled a dramatic shift in the data privacy regime in the United States. With a compliance deadline in 2020, the CCPA grants consumers several new privacy rights. For example, a consumer has the right, subject to certain exceptions, to:

- request that an organisation provide the consumer with access to and certain details about her personal information;
- request that an organisation delete any personal information about the consumer which the organisation has collected from the consumer; and
- direct an organisation not to sell the consumer's personal information.

As such, the CCPA requires covered entities to make significant changes to their privacy programmes concerning how they collect, use and disclose personal information. Since 2018, several legislative proposals seeking to clarify and amend the CCPA have been introduced. Many of these proposed amendments are pending in the California legislature.

Given California's significant economic impact and the fact that the CCPA is the most prescriptive general privacy law in the United States, the law has helped set the stage for several similarly focused proposed laws currently pending in state legislatures. In 2020, California voters passed the California Privacy Rights Act (CPRA), which amends and expands upon the CCPA. In 2021, the Virginia legislature enacted the Virginia Consumer Data Protection Act (VCDPA), making Virginia the second state to enact comprehensive privacy legislation. Both the CPRA and VCDPA's operative provisions will take effect on 1 January 2023. There also is potential for a federal data privacy law. Whether a federal law will pre-empt state laws such as the CCPA also is a topic of debate and disagreement.

Coronavirus

47 | What emergency legislation, relief programmes and other initiatives specific to your practice area has your state implemented to address the pandemic? Have any existing government programmes, laws or regulations been amended to address these concerns? What best practices are advisable for clients?

There is no privacy or security specific law of general application intended to address the pandemic.

HUNTON ANDREWS KURTH

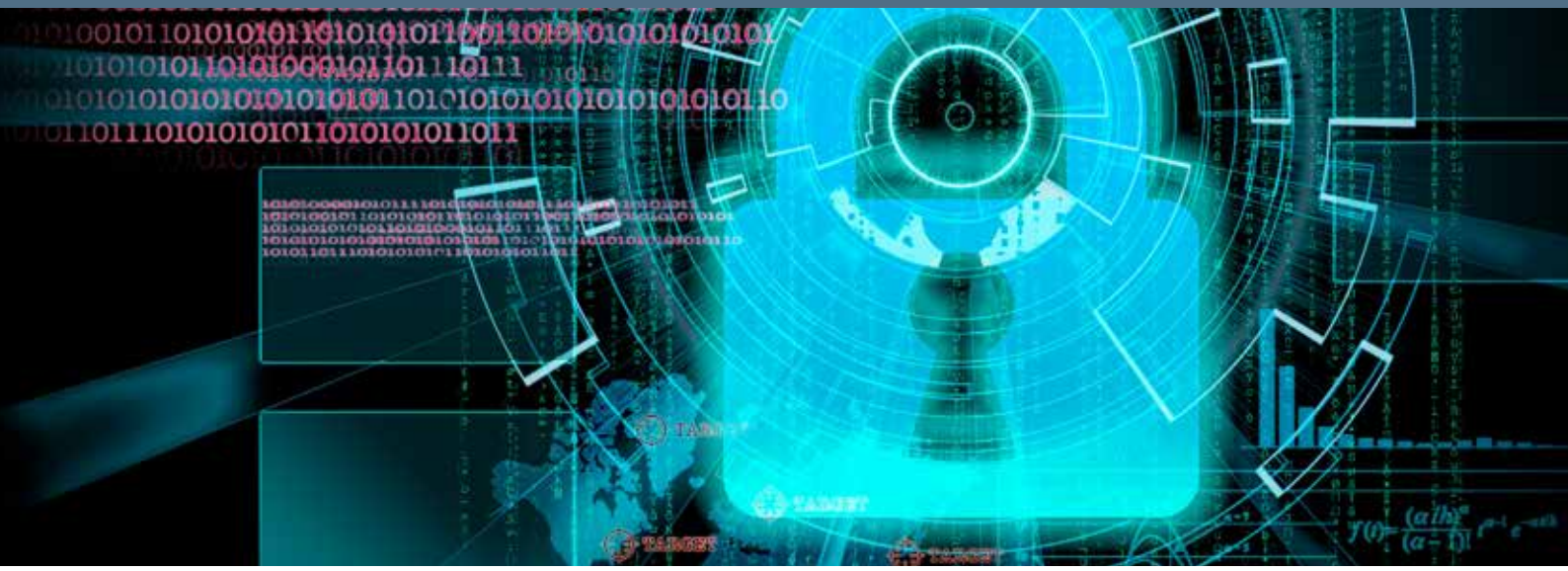
Aaron P Simpson
asimpson@huntonak.com

Lisa J Sotto
lsotto@huntonak.com

200 Park Avenue
New York City
New York
10166
United States
Tel: +1 212 309 1000
www.huntonak.com

HUNTON
ANDREWS KURTH

Leaders in Privacy and Cybersecurity



Keep the trust you've earned.

Complying with global privacy, data protection and cybersecurity rules is challenging, especially for businesses that operate across borders. Our top-ranked privacy team, in combination with the firm's Centre for Information Policy Leadership, advises on all aspects of US and European data protection law and cybersecurity events. We help businesses develop global compliance frameworks addressing regulatory obligations in the US, the EU and across the world. The firm is widely recognized globally as a leading privacy and data security firm.

For more information, visit www.huntonprivacyblog.com.

Other titles available in this series

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Business & Human Rights
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
Drone Regulation
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
Healthcare M&A
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Litigation Funding
Loans & Secured Financing
Luxury & Fashion
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Partnerships
Patents
Pensions & Retirement Plans
Pharma & Medical Device Regulation
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public Procurement
Public-Private Partnerships
Rail Transport
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

lexology.com/gtdt

an LBR business

ISBN 978-1-83862-644-0